**Exercise 12.** *Let $n \geq 2$ be an integer, and let $\mathcal{S}_n$ denote the symmetric group of degree $n$. Let $\varepsilon_1, \ldots, \varepsilon_n$ denote the standard basis of $\mathbf{R}^n$. For each $\sigma \in \mathcal{S}_n$, we define $g_\sigma \in O(\mathbf{R}^n)$ by setting*

$$g_\sigma(\sum_{i=1}^n c_i \varepsilon_i) = \sum_{i=1}^n c_i \varepsilon_{\sigma(i)},$$

*and set $G_n = \{g_\sigma \mid \sigma \in \mathcal{S}_n\}$. Show that $\{s_{\varepsilon_i - \varepsilon_j} \mid 1 \leq i < j \leq n\}$ is precisely the set of reflections in $G_n$. In other words, for $\sigma \in \mathcal{S}_n$, show that $g_\sigma$ is a reflection if and only if $\sigma$ is a transposition.*

*Proof.* We saw earlier that $g_\sigma$ is a reflection if $\sigma$ is a transposition. (See p. 11 of our lecture note.) Next assume $g_\sigma$ is a reflection. Then $g_\sigma^2 = 1$. Since the mapping $\mathcal{S}_n \to G_n$ defined by $\sigma \mapsto g_\sigma$ is an isomorphism, we have

$$\sigma^2 = 1.$$

Therefore there exist $2m$ integers $1 \leq k_1, \ldots, k_{2m} \leq n$ such that

$$\sigma = (k_1\ k_2)(k_3\ k_4) \cdots (k_{2m-1}\ k_{2m}).$$

Without loss of generality, we may assume $k_i = i$ for $1 \leq i \leq 2m$, so that

$$\sigma = (1\ 2)(3\ 4) \cdots (2m-1\ 2m).$$

We need to show that $m = 1$. We give two independent proofs of this.

(1) Since $g_\sigma$ is a reflection, there exists a nonzero vector $\alpha \in \mathbf{R}^n$ such that $g_\sigma = s_\alpha$. For any $1 \leq i \leq m$,

$$s_\alpha(\varepsilon_{2i-1}) = \varepsilon_{2i-1} - \frac{2(\varepsilon_{2i-1}, \alpha)}{(\alpha, \alpha)}\alpha$$

Also since $\sigma = (1\ 2)(3\ 4) \cdots (2m-1\ 2m)$,

$$g_\sigma(\varepsilon_{2i-1}) = \varepsilon_{2i}.$$

Therefore we get

$$\alpha \in \mathbf{R}(\varepsilon_{2i-1} - \varepsilon_{2i}).$$

Since $i$ was arbitrary, this holds for every $1 \leq i \leq m$. But since $\alpha$ is nonzero and $\varepsilon_{2i-1} - \varepsilon_{2i}$ $(1 \leq i \leq m)$ are linearly independent, $m$ must be equal to 1.

(2) For $1 \leq i \leq m$, by the definition of $g_\sigma$, we have

$$g_\sigma(\varepsilon_{2i-1} - \varepsilon_{2i}) = \varepsilon_{2i} - \varepsilon_{2i-1} = -(\varepsilon_{2i-1} - \varepsilon_{2i}).$$

Since $\varepsilon_{2i-1} - \varepsilon_{2i}$ $(1 \leq i \leq m)$ are linearly independent, $g_\sigma$ has an eigenvalue $-1$ with multiplicity at least $m$. On the other hand, since $g_\sigma$ is a reflection, $g_\sigma$ has an eigenvalue $-1$ with multiplicity exactly 1. This proves $m = 1$ as desired. □

**Exercise 13.** *With reference to Exercise 12, set* $\Phi = \{\pm(\varepsilon_i - \varepsilon_j) \mid 1 \leq i < j \leq n\}$ *is a root system, with a positive system* $\Pi = \{\varepsilon_i - \varepsilon_j \mid 1 \leq i < j \leq n\}$*. For* $w \in W(\Phi)$*, setting* $n(w) = |\Pi \cap w^{-1}(-\Pi)|$*, show that*

$$n(g_\sigma) = |\{(i,j) \mid i,j \in \{1,2,\ldots,n\}, i < j, \sigma(i) > \sigma(j)\}| \qquad (\sigma \in \mathcal{S}_n).$$

*Proof.* Fix $\sigma \in \mathcal{S}_n$. By definition, we have

$$\begin{aligned} g_\sigma \Pi &= \{g_\sigma(\varepsilon_i - \varepsilon_j) \mid 1 \leq i < j \leq n\} \\ &= \{\varepsilon_{\sigma(i)} - \varepsilon_{\sigma(j)} \mid 1 \leq i < j \leq n\}. \end{aligned}$$

Since $\varepsilon_{\sigma(i)} - \varepsilon_{\sigma(j)} \in -\Pi$ if and only if $\sigma(i) > \sigma(j)$,

$$g_\sigma \Pi \cap (-\Pi) = \{\varepsilon_{\sigma(i)} - \varepsilon_{\sigma(j)} \mid 1 \leq i < j \leq n, \sigma(i) > \sigma(j)\}.$$

Therefore

$$\begin{aligned} n(g_\sigma) &= |\Pi \cap g_\sigma^{-1}(-\Pi)| \\ &= |g_\sigma \Pi \cap (-\Pi)| \\ &= |\{\varepsilon_{\sigma(i)} - \varepsilon_{\sigma(j)} \mid 1 \leq i < j \leq n, \sigma(i) > \sigma(j)\}| \\ &= |\{(i,j) \mid 1 \leq i < j \leq n, \sigma(i) > \sigma(j)\}|. \end{aligned}$$

The result follows.

□